REMARKS

The Examiner has objected to claims 1-8, 14-29 and 35-58 on the basis that their status was shown as "withdrawn". The applicant has amended the claims to indicate their status as "cancelled".

The Examiner has objected to claims 9-13 and 30-34 on the basis that the claims are directed to nonstatutory subject matter. The applicant traverses this objection.

Having regard to claims 9-13, there is provided a split-mask, masking countermeasure method for improving the resistance, to power analysis attacks, of a processing unit performing a defined cryptographic function using a key. The applicant submits that the method is tied to a processing unit performing a defined cryptographic function using a key. By implementing the claimed method, power levels in the processing unit are affected such that a power analysis attack on the unit, a physical measurement of the power levels (e.g. a voltage measurement), will be frustrated.

The applicant submits that claims 9-13 are statutory as they are: a) tied to a processing unit performing a defined cryptographic function using a key; and, b) transform the processing unit performing a defined cryptographic function using a key by altering the resultant power levels to render the processing unit resistant to a power analysis attack. The method alters the operation of the processing unit to change the power levels it emits when it is performing the defined cryptographic operation.

Having regard to claims 30-34, the applicant submits that the claims as previously amended limited the computer program product to one embodied in storage media. As quoted by the Examiner, page 10, lines 1-4 of paragraph 43 specifically distinguish between: "signals carried by networks, including the Internet or may be embodied in media such as magnetic, electronic or optical storage media. The applicant submits that the claim as previously amended was in fact limited to exclude signals. The applicant has made a further amendment to clarify this by replacing the term "embodied" with "stored".

The Examiner has rejected claims 9-13 and 30-34 as being unpatentable over Kocher (US 6,278,783) in view of Moyse (US 5,446,651). The applicant respectfully traverses this rejection.

In particular, Kocher does not disclose at least elements (3), (5), (6) and (7) as listed by the Examiner. As previously explained, Kocher does not disclose "split masks". Further, Kocher does not disclose a split mask value mn to be r^min1^...^minn^m1^...^mn-1 as stated by the Examiner. The sections cited by the Examiner (Figure 2; column 7, lines 30-33; column 8, lines 31-51) do not, as claimed by the Exmanier, disclose key splitting.

As previously explained, Kocher is directed towards a masking and permutation scheme for making DES-type cryptography resistant to attack. The scheme involves replacing the key K with a random mask value K1 and a masked key K2, related to K by the relationship K2 = K XOR K1. In Kocher, the masked key K2 is the original key K as masked by the random mask K1. The masked key K2 and mask K1 are also permuted, with random permutations created K2P and K1P. Thus, there is no splitting of the key, only masking of a key K to produce a masked key K2.

The use of key masking, K2 = K XOR K1, is well known in the art of cryptography. Kocher has added the element of using a permutation of K2, K2P and K1, K1P in the cryptographic operation to improve the resistance of the algorithm to cryptographic attack.

In summary, Kocher protects various values, such as the key K, using a straight masking operation (K2 = K XOR K1) so that a masked version of the value, in this case masked key K2, as permutated to K2P, and the mask K1, as permutated to K1P, is used in the cryptographic operation.

The present application is directed towards a method for protecting the key and key mask by using replacement values in the cryptographic operation in place of the key and key mask. The present application achieves this by using split masks, where the split masks are defined with reference to random values used in the masking operation, so that in the operation each encryption operation using the same key only the split mask values m1, m2, ...mn and masked

key mkey are used in the operation. The key mask r is not directly applied or used in the cryptographic operation. Accordingly, measurements of the cryptographic operation through a power analysis attack will not yield the key value or the key mask value r.

To compare with Kocher, mkey is roughly equivalent to K2 and the key mask value r is roughly equivalent to K1. Unlike Kocher, however, r, or a permutation of r, <u>is not used</u> in the cryptographic operation. Instead, split mask values are used, where mn is defined in relation to r, such that the r is indirectly a component of the cryptographic function.

Kocher, only discloses using a permutation of K1 in the cryptographic operation. There is no disclosure in Kocher of using split masks, where mn is defined in relation to r, in the cryptographic operation.

Accordingly, the Examiner's argument that Kocher discloses defining a value mn, or obtaining a set of random values m1, ...mn-1, is incorrect. Kocher employs a permutation of K1, K1P, in the operation and does not generate a split mask defined in relation to the key mask value. The applicant would further argue that other aspects of the claim are distinguishable over Kocher. For instance, Kocher does not disclose obtaining a set of n random input values, to be used in masking a defined cryptographic function or generating a mask table.

The Examiner further argues that Moyes discloses "the capability of splitting mask value". The applicant respectfully disagrees. Moyes is directed towards a split multiply operation. Column 29 lines 25-39 deals with arithmetic logic unit operations that specify multiple operation. In the context of such operations, the term "mask" is being used as a computer science term to describe data that is used for bitwise operations, that is computer arithmetic. The section cited by the Examiner is not related to cryptography, but to mathematical operations being performed by a bitwise operation (see http://en.wikipedia.org/wiki/Mask_(computing)). While the section includes the terms "mask" and "split", they are being taken out of context within a 100+ page patent disclosure directed towards a multiplication apparatus. The applicant submits that Moyes does not disclose splitting a mask as the term would be understood in cryptography.

Favourable consideration and allowance of this application are respectfully requested.

Executed at Toronto, Ontario, Canada, on February 25, 2010.

Catherine Helen Gebotys

Etienne P. de Villiers
Registration No. 58632
(647) 288-9537
Customer Number: 38735